

Serial No. 09/468,377
Art Unit No. 2134

REMARKS

Claims 1-17 are currently pending in the patent application. The Examiner has rejected Claims 1, 5, 12, 13, 15 and 16 under 35 USC 103 as unpatentable over the teachings of Thomlinson in view of Shi; Claims 2 and 6 as unpatentable in view of Thomlinson in view of Shi and Danneels; Claims 3 and 7 as unpatentable over Thomlinson in view of Shi and Buck; Claims 4 and 8 as unpatentable over Thomlinson in view of Shi and the IBM TDB; Claims 9-11, 14, and 17 as unpatentable over Jablon in view of Thomlinson; and, Claim 11 as being unpatentable over the teachings of Jablon and Thomlinson in view of Schneider. For the reasons set forth below, Applicants respectfully assert that all of the pending claims, as amended, are definite and patentable over the cited prior art.

Applicants note that the present invention expressly recites a method for securely providing data of a content provider to a user without trusting an internet service provider, said method comprising a. generating a first key known only to said content provider; b. encrypting a second key using said first key and an encryption algorithm

YO999-558

-10-

Serial No. 09/468,377
Art Unit No. 2134

requiring a one-time password or requiring a one-time password and a separate user provided password; c. storing said encrypted second key on a client machine; and when said user desires to access said data, d. decrypting said second encrypted key using the first key or the user provided password; and e. accessing said data using the second key (independent Claims 1, 5, 12, 15, 13, and 16, and claims 2-4 and 6-8 which depend therefrom). All of those claims have been rejected based on the Thomlinson patent as a primary reference.

The Thomlinson patent is directed to a system and method for protecting data wherein the service provider is involved in the encryption and authentication process. Applicants respectfully assert that the present invention expressly omits the service provider from the process in order to protect data when an untrusted service provider is part of the data delivery. Further, the Thomlinson keys are reversed from that which is taught and claimed by the present invention. Whereas Thomlinson uses a first master key to encrypt a second item key, and then uses the first master key to decrypt the second key for a user to access the item data, the present invention does not use the second

YO999-558

-11-

Serial No. 09/468,377
Art Unit No. 2134

key to encrypt stored items. Rather, the present invention creates the second key and stores that encrypted second key at the client machine.

As noted by the Examiner, the Thomlinson patent does not teach or suggest storing encrypted second keys at the client. What the Examiner says is that the cookies created and stored at the client in the Shi patent render that claim feature obvious. Applicants respectfully assert that cookies are not the same as or suggestive of an encrypted second key which is encrypted using a first key known only to the content provider and is sent for storage at a client. A cookie is a non-unique, non-encrypted, fully accessible set of data which can be replicated on any client machine which accesses a server. Storing a cookie is unworkable for an authentication system in which access is to be limited. Moreover, even if one skilled in the art were to modify Thomlinson with the Shi cookies, one would not arrive at the present invention.

The other primary reference, Jablon, provides a scheme in which two trusted parties each generate a unique code and share it. The Jablon patent does not, however, teach or suggest the particular code generation scheme which is

YO999-558

-12-

Serial No. 09/468,377
Art Unit No. 2134

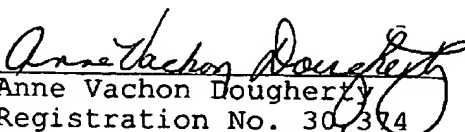
taught and claimed by the claims including 9-11 and 14 and 17. The claims are not drawn to "a method wherein two parties operate on the same code element", but are quite specific to the implementation claimed. Accordingly, Applicants believe that the Jablon teachings do not obviate the invention as claimed.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

Y. Baransky, et al

By:


Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910

YO999-558

-13-